REMARKS/ARGUMENTS

Reconsideration and allowance of this application are respectfully requested. Currently, claims 2-8 and 23-24 are pending in this application.

Rejection Under 35 U.S.C. §112:

Claims 1-14 and 16-22 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Claims 1, 9-14 and 16-22 have been canceled and claims 2-8 now depend from new claim 23. Applicant submits that new claim 23 and its dependents are in full conformance with 35 U.S.C. §112, first paragraph. In particular, claim 23 is supported by, for example, page 11, line 3 to page 14, line 18 and Figs. 7-8 of the originally-filed application.

Claim 23 relates to a method of operating an authenticating server system for authenticating a user of a client application provided on a client terminal of the type such as T3 in the specification. As described in the specification, terminals of the type T3 cannot be identified by their own IP address. To promote understanding of the invention, a description of an exemplary (but in no way limiting) embodiment described in the above-identified portion of the specification is provided below.

A user at such a terminal logs on to the server system via an application server APS designated as an authentication server (see page 11, lines 3 to 5). An application client APC (e.g., a WWW browser) sends document request over the network in order to access the APS.

When the APC sends this request, it provides a cookie to the APS. Initially, this cookie will not contain any information (i.e., no address token (validated or unvalidated) is included) enabling the user to be identified (see page 12, lines 17-23 of the specification). When such a cookie is received by the APS, it sends a cookie to the APC which contains an unvalidated address token (see page 12, lines 8-10 and 22 of the specification).

When the APC receives the unvalidated address token, it stores the unvalidated address token and prompts the user for a username and password. The APC then returns the unvalidated address token along with the username and password (hashed by the secure password client SPC for the client application) in a cookie to the APS. The APS receiving this information functions passes this information on to the cache management server CMS which polls the secure password server database 8 to determine if the username and password hash match one stored in the SPS database 8.

If the information provided indicates the user is authenticated etc., then the CMS retrieves the user's access rights token 8 from the SPS store 8. If authenticated, the CMS then generates an access allowed message and stores the validated address token and authenticator information (e.g., the password and username hash) for the user and the access rights token in the CMS store 10.

If an access allowed message is generated, then the APS sends the requested document, along with an updated cookie containing the new *validated* address token and the username and password hash, which is then stored at the client terminal.

Subsequent document requests will contain only the validated address token and username and password hash, which avoids the need to repeat the authentication process each time the user requests a new document. The address token itself uniquely identifies the user terminal.

There are therefore three stages to the authentication process performed at the application server functioning as the authentication server in the exemplary embodiment of the invention where a client terminal of the network cannot be identified using its unique IP address: (i) if no address token is present, then one is created, (ii) if an unvalidated address token is present, it is validated, and (iii) if a validated address token is sent (with subsequent requests), it is used to validate document requests.

Applicant therefore submits that all of the pending claims are in full conformance with 35 U.S.C. §112, first paragraph.

Rejections Under 35 U.S.C. §103:

Claims 1-4, 8-11, 13 and 15-19 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Levergood et al (U.S. '780, hereinafter "Levergood") in view of Kirsch (U.S. '915). Claims 5-7, 12 and 14 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Levergood in view of Kirsch and further in view of See et al (U.S. '243, hereinafter "See"). Applicant submits that new independent claim 23 and its dependents are not "obvious" over Levergood in view of Kirsch or Levergood in view of Kirsch and in further view of See. Applicant therefore requests that the rejections under 35 U.S.C. §103 be withdrawn.

In order to establish a prima facie case of obviousness, all of the claimed limitations must be taught or suggested by the prior art. Applicant submits that the combination of Levergood in view of Kirsch fails to teach or suggest all of the claimed limitations. For example, the combination fails to teach or suggest performing at a resource server, if no address token which uniquely identifies the user is contained in client-side persistent information accompanying a document request, generating and transmitting a address token which uniquely identifies the user without prior receipt at the resource server of a previously issued address token which uniquely identifies the user.

For terminals which cannot be identified by their own IP address, a resource server (an application server) in the present invention essentially (in addition to other functions) acts as an authentication server by responding to a document request received from a client application running on the terminal by providing an address token which uniquely identifies the user. Initially, the resource server does not have any unique user name or password information from the user or an IP address from the user's terminal. An address token which uniquely identifies the user is thus transmitted from the resource server to the client terminal without the resource server having previously received any unique identifier of the user or the user's terminal.

In contrast, neither Kirsch nor Levergood teaches providing an initial address token to function as a unique identifier prior to receiving any user name/password information. Both Kirsch and Levergood disclose generating an identifier (either a session identifier (SID) in Levergood or cookie information in Kirsch) which

incorporates some unique identifier for the user. However, this unique identifier in Levergood and/or Kirsch is generated only after certain information has been received from the user (either an IP address of the requesting terminal as in Levergood or, for example, an identifier which incorporates the user name/id and password information as in Kirsch). Neither Kirsch nor Levergood therefore teaches or suggests a resource server generating and transmitting to a terminal, which cannot be identified by its own IP address, an address token which uniquely identifies the user without prior receipt of a uniquely identifying address token as required by the claimed invention. See fails to remedy this deficiency of Kirsch and Levergood.

The combination of Kirsch and Levergood also fails to teach or suggest three possible stages of an authentication process performed at a resource server including: a first process in which if no uniquely identifying address token is received, such an address token is generated and transmitted (see (i) in claim 23); a second process in which if an unvalidated address token is received, the unvalidated address token is validated (see (ii) in claim 23); or a third process in which if a validated address token is received, the validated address token is used to validate a document request (see (iii) in claim 23). Again, See fails to remedy these deficiencies of Kirsch and Levergood.

Levergood discloses an internet server access control and monitoring system in which the following steps occur:

i) a client request is made to a URL;

ii) if no session identification (SID) is appended to the request, the Internet server subjects the user to an authorization routine ***prior to issuing the SID***; and

iii) if a session identification is appended to the request, a content server validates the SID.

This authorization routine noted in (ii) includes the following steps:

(a) The content server initiates the authorization routine by ***redirecting*** *the client's request to an authentication server which may be a different host.*

(b) The authentication server then returns a response to interrogate the client.

(c) If the client is qualified, the authentication server issues a SID to the client.

A client must already be "qualified" prior to the SID being issued according to Levergood. In contrast, according to the invention, the address token (used as an identifier) is issued to any user, whether "qualified" or not (see, e.g., Figure 7 of the application and contrast with Figure 2 of Levergood).

In Levergood, it is necessary for the SID itself to contain the IP address of the user's computer as well as possibly hashed information from the user. While an alternative embodiment of Levergood (see col. 4, lines 24 to 28) describes how server access control can be maintained by programming the client browser to store a SID or similar tag for use in each URL call to that server, this would require a specialized browser (see col.4, lines 28 to 31). Finally, in Levergood the receipt of a request by a content server is redirected *via the originating client browser 100* (see Figure 2) to the authentication server 200. In contrast, in the present invention, a resource server (a

resource server from which the document is requested) essentially functions at least at one point as the authentication server. Levergood thus fails to teach the resource server functioning as an authentication server and generating an address token which uniquely identifies the user and which is sent to the client terminal in response to receiving a request for a document from the client terminal which does not contain anything to uniquely identify the user/terminal. Neither Kirsch nor See resolves these deficiencies of Levergood.

Kirsch relates to the different field of internet purchase transactions. Kirsch teaches that a persistent predetermined coded identifier can be established on a client browser corresponding to an account record stored by the merchant server. In Kirsch, server-1 (22) receives a URL request/web page service transaction T1 from a client browser and in response serves web page 24 to the client browser. The returned web page enables the user to make further requests which may or may not be from the same server (see Figure 2, col. 7, lines 25-42). If a purchase request is then made, the purchase URL selected by the user prompts the appropriate server (server-2 (34)) to negotiate and establish a secure session T2 with the browser (col. 7, lines 55-56). Any **client-side stored** cookie information data corresponding to the request URL is also passed to Server-2 (see col. 7, lines 58 to 60).

If the user has an authenticated credit relationship already established with server-2, the client-side cookie encodes information sufficient to re-authenticate the client user to the server-2. If not, then such a cookie will not exist on the client system, and server-2

initiates a process to establish such a credit relationship with the client. This is done by server-2 sending the client a form, and only when a response is received from the client does server-2 create a cookie which is sent to the client incorporating information from the form the user has completed. This cookie is then used in connection with **subsequent** URL purchase requests. Server-2 creates a database record in database 36 only **after** the user has returned sufficient information for it to create a cookie (see col. 7, lines 65 to Col. 8, lines 4, lines 7 to 12).

As discussed above, Levergood discloses an SID which is issued only **after** the user has been authenticated. Even if Kirsch and Levergood were combined as proposed by the Office Action, the combination would not have taught or suggested all of the claimed limitations. See also fails to remedy the deficiencies of Levergood and Kirsch. Applicant thus requests that the rejections under 35 U.S.C. §103 be withdrawn.

Conclusion:

Applicant believes that this entire application is in condition for allowance and respectfully requests a notice to this effect. If the Examiner has any questions or believes that an interview would further prosecution of this application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

Raymond Y. Mah
Reg. No. 41,426

RYM:sl
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4044
Facsimile: (703) 816-4100